MOBILE SICHERHEIT HINKT HINTERHER

Der einfachste Weg ins Unternehmensnetzwerk ist, ein Mobilfunkgerät zu kapern. Die mobile Revolution eröffnet Cyberkriminellen neue Angriffsmöglichkeiten. Organisationen erkennen, dass «Bring Your Own Device» zwar die Produktivität erhöht, doch viele Unternehmen ergreifen nicht die richtigen Massnahmen, um sich effektiv zu schützen.

→ **VON SONJA MEINDL**

Smartphones und Tablets sind die Träger der Digitalisierung. Keine anderen Endpunkte versinnbildlichen die vernetze Welt so sehr wie mobile Geräte: Sie sind 24 Stunden online, machen Unternehmensressourcen überall verfügbar und haben den Arbeitsalltag in fast allen Organisationen grundlegend verändert. Mobilgeräte in Unternehmen sind Fluch und Segen zugleich. Fluch, was den Zugriff betrifft, und Segen für die Unternehmensproduktivität. E-Mails im Zug oder Tram checken, Applikationen von unterwegs aus herunterladen – alles kein Problem im digitalen Zeitalter. Leider schlummert in den handlichen Mini-Computern aber auch eine erhebliche Gefahr.

Nicht nur unsere Security Reports, auch eine internationale Studie von Dimensional Research bestätigt das bestehende Sicherheitsrisiko. Cyberkriminelle wissen, dass mobile Endpunkte ein leicht ausnutzbarer Angriffsvektor sind und konzentrieren sich gezielt darauf. Ihre Zahl wächst unaufhörlich und Sicherheitsverantwortlichen fällt es immer schwerer, den Überblick zu behalten.

Neben firmeneigenen Smartphones und Tablets bewegen sich auch Geräte der Mitarbeiter (BYOD) in den Netzwerken. Deren Absicherung ist kein leichtes Unterfangen. Sicherheitswerkzeuge und Prozesse müssen alle Geräte erfassen und verwalten, da Angreifer immer gezielt nach dem schwächsten Glied in der Kette suchen – und das ist oft ein privates Device.

VIEL NACHHOLBEDARF BEI MOBILER SICHERHEIT

Zahlreiche Mechanismen müssen daher angepasst werden: Zwei Drittel der in der Studie befragten Sicherheitsbeauftragten fühlen sich nicht ausreichend gegen die mobile Bedrohung gewappnet. Zeitgleich ändert sich die Bedrohungslage und man geht von einem deutlichen Anstieg der Angriffe schon innerhalb dieses Jahres voraus. Ein Fünftel aller Organisationen gibt sogar an, bereits Opfer einer mobilen Attacke geworden zu sein.

Die Dunkelziffer dürfte gleich aus zwei Gründen höher liegen. Einerseits möchte man nicht als angreifbar gelten und spricht nach der Entdeckung nur ungern über eine erfolgreiche Cyberattacke. Zudem fehlt vielen IT-Abteilungen die Fähigkeit zur Erkennung von ungewöhnlichen Vorgängen. 24 Prozent können nicht sagen, ob es einen Sicherheitseinbruch auf diesem Gebiet gegeben hat. Das klingt nach viel Nachholbedarf. Tatsächlich bestätigen nur knapp 38 Prozent der 410 Befragten, eine entsprechende Sicherheitslösung einzusetzen, die über Enterprise Mobility Management (EMM) hinausgeht.

BEDROHUNG KENNT VIELE GESICHTER

Die Sicherheitsverantwortlichen berichten von einem breiten Spektrum von Angriffstypen. An der Spitze befindet sich mit 58 Prozent Malware, dicht gefolgt von Phishing via SMS (54 Prozent). Gleichauf liegen Netzwerkattacken über infizierte Wi-Fi oder Man-in-the-middle-Exploits. Knapp über 40 Prozent beanspruchen abgefangene Anrufe und Textnachrichten über ein Mobilfunknetz sowie Zugangsdatendiebstahl und Key Logging. Vor diesem Hintergrund wundert es niemanden, dass fast 80 Prozent der Studienteilnehmer die Aufgabe, mobile Geräte zu schützen, für immer schwieriger halten.

Beispiele gibt es leider viele. Im letzten Jahr sorgte HummingBad für Schlagzeilen. Die Malware installiert sich über infizierte Play-Store-Apps und manipulierte Webseiten. HummingBad erstellt einen permanenten Rootzugriff auf dem Endgerät des Opfers und kreiert Einnahmen durch manipulierte Klicks auf Bannerwerbung. Zusätzlich kann durch die Malware weiterer Schadcode eingeschleust werden, um beispielsweise Informationen auch aus geschützten Bereichen zu extrahieren. Weltweit kam es zu über 85 Millionen nachgewiesenen Infektionen.

HOHE SCHADENSUMMEN

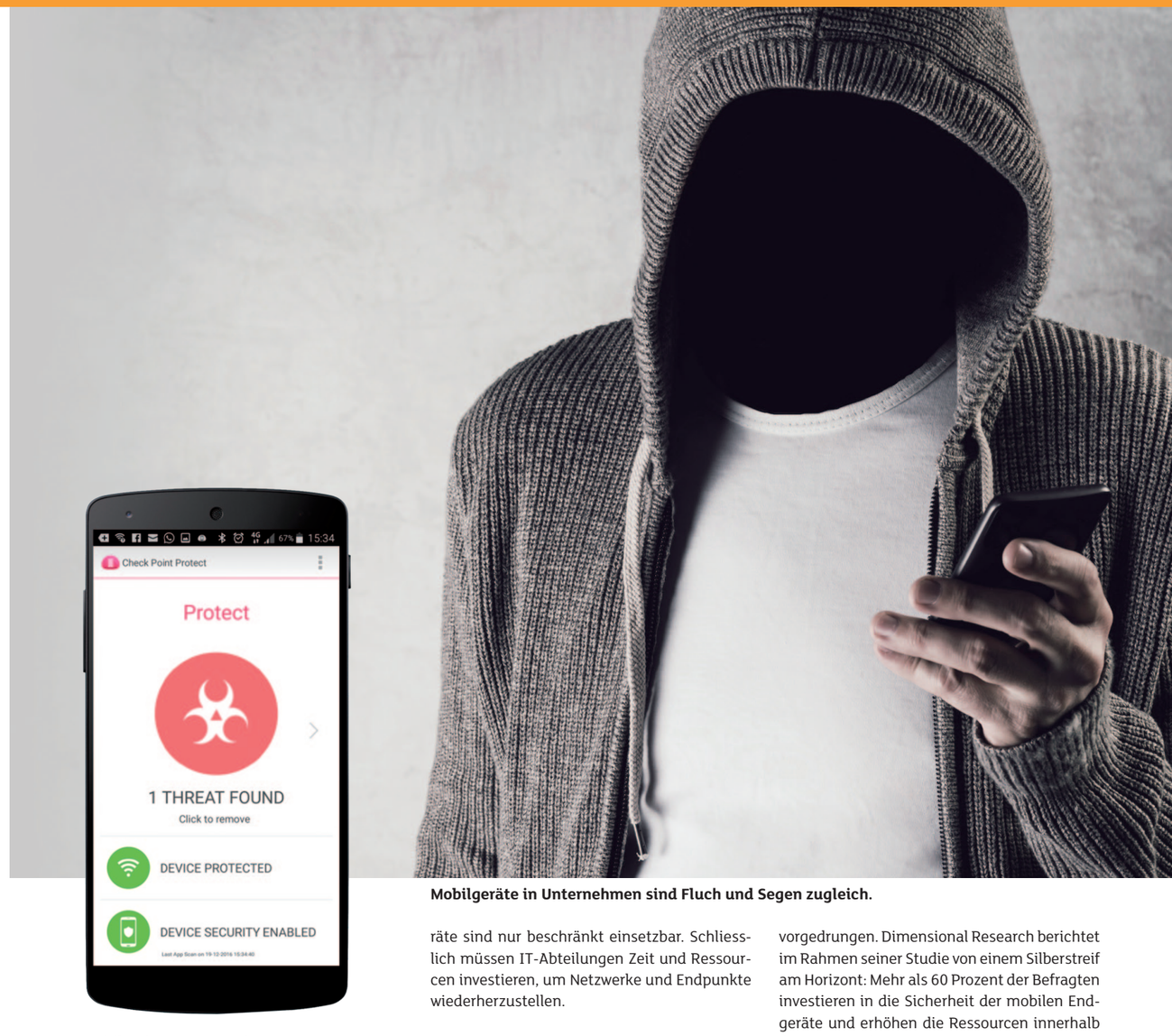
Viele IT-Verantwortliche unterschätzen den Schaden infolge eines mobilen Sicherheitseinbruchs, er steht denen eines herkömmlichen Vorfalls über Desktop-PC oder Notebook in nichts nach. 37 Prozent setzen die finanziellen Folgen für das eigene Unternehmen bei mehr als 100'000 USD an, 23 Prozent schätzen die Kosten über eine halbe Million USD. Zum einen resultieren diese hohen Summen aus den entwendeten Informationen, Firmengeheimisse sind unwiederbringlich verloren. Weiter können Angestellte nicht weiterarbeiten oder die Geräte sind nur beschränkt einsetzbar. Schliesslich müssen IT-Abteilungen Zeit und Ressourcen investieren, um Netzwerke und Endpunkte wiederherzustellen.

MOBILE DEVICE MANAGEMENT SYSTEM REICHT NICHT AUS

Entsprechende Abwehrlösungen müssen alle Bedrohungsvektoren im Blick behalten: auf dem Gerät, in den Anwendungen und im Netzwerk. IT-Teams in Unternehmen stehen vor einer doppelten Herausforderung. Die User-Experience besitzt einen hohen Stellenwert. Fällt die Lösung eines Unternehmens zu restriktiv aus, suchen sich die Mitarbeiter schnell andere Wege, ihre Arbeit zu erledigen. Trotzdem sind IT-Verantwortliche verpflichtet, Endpunkte und Netzwerke zu schützen und Sicherheitseinbrüche zu unterbinden.

Deshalb machen im Bereich Smartphones und Co. minimalinvasive Schutzkonzepte Sinn. IT-Sicherheitsspezialisten ist schon lange klar, wie viel Nachholbedarf auf diesem Gebiet besteht. Inzwischen ist die Problematik um die Mini-Computer auch bis in die Führungsetagen vorgedrungen. Dimensional Research berichtet im Rahmen seiner Studie von einem Silberstreif am Horizont: Mehr als 60 Prozent der Befragten investieren in die Sicherheit der mobilen Endgeräte und erhöhen die Ressourcen innerhalb dieses Bereichs.

Umfassende mobile Sicherheit muss sich gegen System-Probleme, Root-Zugriffe, Konfigurationsänderungen, gefälschte oder bösartige Apps und Trojaner sowie Malware und Netzwerkangriffe wappnen. Ein Mobile Device Management (MDM)-System reicht nicht aus. Ein umfassendes Sicherheitsmanagement erfordert eine modulare Bauweise. Insbesondere sichere Container zur Verhinderung von Datenverlust zwischen beruflich und privat genutzten Anwendungen auf dem gleichen Device sowie Mobile Threat Prevention-Lösungen zum Schutz vor bösartigem App-Verhalten sind unverzichtbar. ←



Mobile Threat Prevention-Lösungen zum Schutz sind unverzichtbar.

Mobilgeräte in Unternehmen sind Fluch und Segen zugleich.

Zur Autorin

Sonja Meindl ist diplomierte Wirtschafts-Ingenieurin und verantwortet als Country Manager seit 2012 die Geschäfte von Check Point in der Schweiz und in Österreich.

Zum Unternehmen:
Check Point Software Technologies ist der grösste Pure-Play Netzwerk- und Cybersicherheitsanbieter weltweit. Als Marktführer der Cybersicherheitsbranche bietet Check Point die führende Technologie und schützt seine Kunden vor Cyberattacken; mit einer unschlagbaren Fangquote bei Malware und anderen Bedrohungen. Check Point bietet eine umfassende Sicherheitsarchitektur, um Unternehmen zu schützen. Egal, ob Netzwerk oder Mobilgerät – Check Point deckt alle Bereiche ab und kann diese über seine leicht verständliche Sicherheitsmanagementplattform verwalten. Über 100'000 Organisationen vertrauen auf den Schutz von Check Point. Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt mehr als 30 Mitarbeitende

Mehr Informationen:
www.checkpoint.com

Check Point SOFTWARE TECHNOLOGIES LTD.

Dieser Beitrag wurde von **Check Point Software Technologies** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.